UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,321	03/02/2004	Christopher N. Kline	END920030127US1	1828

68786 7590 02/19/2008
CHRISTOPHER & WEISBERG, P.A.
200 EAST LAS OLAS BOULEVARD
SUITE 2040
FORT LAUDERDALE, FL 33301

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
02/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,321	KLINE, CHRISTOPHER N.	
	Examiner	Art Unit	
	Amare Tabor	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to REMARKS filed on November 29, 2007.

2. Claims 1-17 are pending.

Response to Arguments

3. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Specification

4. The disclosure is objected to because of the following informalities:

- Page 9: lines 3-4 discloses, "*in the illustrated embodiment, a person with application-level or system-level super user privilege maintains list **54***"; and lines 9-10 discloses, "*in the illustrated embodiment, a person with application-level or system-level super user privilege maintains list **58***." Please correct or clarify how 54 and 58 could maintain identical lists.
- Page 10: lines 12-14 discloses, "*After steps 110 and 112, the privilege checking program 50 **loops back** to repeat the foregoing analysis and report for the next group*"; However, this loop is not shown in FIG. 2A. Please correct or clarify.
- Page 11: line 8 discloses, "*The operating system obtains these names from the master configuration file **50**.*" However, according to FIG. 1, the master configuration file is 22. Please correct or clarify.
- In pages 11-12, "*program*" 60 of FIG. 1, is disclosed as "*application authority manager program.*" Please correct or clarify.

Claim Objections

5. Claim 3, 5 and 14 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The functions of the fourth instructions in Claims 3 and 5 are already covered by the second/third instructions of Claim 1; and similarly, functions of the fourth instructions in Claim 14 are already covered by the second/third instructions of Claim 11.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 3, 5, 11 and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 1, 3, 5, 11 and 14 are rejected under 35 U.S.C. 112, 2nd paragraph as being unclear.

- Claim 1 recites the limitation, "*third program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege*";
- Claim 11 recites the limitation, "*third program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege*";
- Claims 3 recites the limitation, "*fourth program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege*";

- Claim 5 recites the limitation, "*fourth program instructions to determine if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list*"; and

- Claim 14 recites the limitation, "*fourth program instructions to determine if all the members of said group with the higher actual privilege having a group name not generally used for a group with higher level privilege are on the list of trusted individuals.*"

Examiner contacted Applicant's Attorney (on 01/30/2008) seeking an explanation what the third (and fourth) program instructions of Claims 1 and 11 (and Claims 3, 5 and 14) is (are) performing. Examiner would like to thank the Attorney for the prompt answer; however, Examiner still could not understand what the third (and fourth) program instructions in Claims 1 and 11 (and Claims 3, 5 and 14) is (are) performing explicitly. Applicant is required to explain further or amend the functions of the third (and fourth) instructions.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art, referred as "*AAPA*" hereinafter in view of Ashland et al. (US 7,219,234 B1), referred as "*Ashland*" hereinafter.

As per Claim 1, AAPA discloses,

first program instructions to compare members within each of said groups to a list of trusted individuals (page 2, lines 26-28, "*An administrator occasionally reviewed the members of privileged groups to determine if the administrator knew, through personal knowledge, that the members were all trusted individuals*");

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals; and third program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege (page 2, lines 18-20, "*The system administrator would review the privilege level for each group name to determine if the group names typically used for user groups (as known by the system administrator) have higher than "user" level privilege")*;

generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; and generate a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted (page 2, lines 16-18, "*It was previously known for a system administrator to periodically, manually enter commands into the computer to output the group names and their privilege levels to a text file*").

AAPA does not explicitly disclose computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: a computer readable medium; and wherein said first, second and third program instructions are recorded on said medium.

However, Ashland discloses computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: a computer readable medium; and wherein said first, second and third program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claim 6, AAPA discloses,

means for comparing members within each of said groups to a list of trusted individuals (page 2, lines 26-28, "*An administrator occasionally reviewed the members of privileged groups to determine if the administrator knew, through personal knowledge, that the members were all trusted individuals*");

means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals; means for determining if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege (page 2, lines 18-20, "*The system administrator would review the privilege level for each group name to determine if the group names typically used for user groups (as known by the system administrator) have higher than "user" level privilege")*;

and if so, generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; and generate a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted

(page 2, lines 16-18, "*It was previously known for a system administrator to periodically, manually enter commands into the computer to output the group names and their privilege levels to a text file*").

AAPA does not explicitly disclose computer system for determining if any of a plurality of groups may have an improper actual level of privilege. However, Ashland discloses computer system for determining if any of a plurality of groups may have an improper actual level of privilege (see *abstract and FIG.1-2 and 4-5*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claim 11, AAPA discloses,

first program instructions to compare members within each of said groups to a list of trusted individuals (page 2, lines 26-28);

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals; and third program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (page 2, lines 18-20);

and if so, generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; generate a report that said group with the higher actual privilege level has a group name not generally used for a group with the higher level privilege, such that the members of said groups with the higher actual privilege having a

group name not generally used for a group with the higher level privilege are revealed as trusted or not trusted (page 2, lines 16-18).

AAPA does not explicitly disclose computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: a computer readable medium; and wherein said first, second and third program instructions are recorded on said medium.

However, Ashland discloses computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: a computer readable medium; and wherein said first, second and third program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5*)..

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claim 15, AAPA discloses,

first program instructions to compare members within each of said groups to a list of trusted individuals (page 2, lines 26-28);

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (page 2, lines 18-20);

and if so, remove said member not on the list of trusted individuals from said group (page 2, lines 20-21, "*Such case would warrant further investigation" Depending on the outcome of the investigation, the system administrator may remove a member*).

AAPA does not explicitly disclose a computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium.

However, Ashland discloses computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claim 16, AAPA discloses,

first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege or no privilege; and second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with user level privilege or no privilege, to compare members of such group to a list of trusted individuals (page 2, lines 18-20 and 26-28);

and if any member(s) of such group do not appear on said list of trusted individuals, remove said member(s) from such group that do not appear on the said list of trusted individuals (page 2, lines 20-21).

AAPA does not explicitly disclose a computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium.

However, Ashland discloses computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claim 17, AAPA discloses,

first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege; and second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, to compare members of such group to a list of trusted individuals (page 2, lines 18-20 and 26-28);

and if any member(s) of such group do not appear on said list of trusted individuals, lower the actual privilege level of said group (page 2, lines 20-21; *Depending on the outcome of the investigation, the system administrator may lower the privilege level of the group*).

AAPA does not explicitly disclose a computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium.

However, Ashland discloses computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; and wherein said first and second program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification would be obvious because one having ordinary skill in the art would be motivated to automate the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead (see *BACKGROUND OF THE INVENTION*).

As per Claims 2, 7 and 12, combination of AAPA and Ashland disclose,

wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances (see *FIG.4-6 of Ashland; different privilege levels are assigned to members in a group);*

and said third program instructions makes its determination separately for each application or application instance (see for example, *Step 704 of FIG. 7 of Ashland; where create at least one ACR, each having one or more entities, each entry to associate one or more groups and/or one or more userids with a respective set of access rights is disclosed*); and

means for determining if any group with an actual privilege level higher than user level privilege has a group name generally used for a group with user level privilege makes its determination separately for each application or application instance (see *Administrator in AAPA*).

As per Claims 3 and 8, combination of AAPA and Ashland disclose,

fourth program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (page 2, lines 18-20 of AAPA);

and if so, generate a report that said group with the higher actual privilege level has a group name not generally used for a group with the higher level privilege, such that the members of said groups with the higher actual privilege having a group name not generally used for a group with the higher level privilege are revealed as trusted or not trusted (page 2, lines 16-18 of AAPA); and

means for determining if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (see *administrator in* page 2, lines 18-20 and 26-28 of AAPA).

and wherein said fourth program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5 of Ashland*).

As per Claims 4, 9 and 13, AAPA discloses,

wherein said second program instructions determine if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals (page 2, lines 18-20 and 26-28);

and means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals determines if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals (see *administrator in* page 2, lines 18-20 and 26-28);

and if so, generate a report that said group with the higher actual privilege level has all its members on the list of trusted individuals (page 2, lines 16-18).

As per Claims 5, 10 and 14, combination of AAPA and Ashland disclose,

fourth program instructions to determine: if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list of trusted individuals; if all the members of said group with the higher actual privilege having a group name not generally used for a group with higher level privilege are on the list of trusted individuals (page 2, lines 18-20 and 26-28 of AAPA);

and means for determining if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list of trusted individuals (see *administrator in* page 2, lines 18-20 and 26-28 of AAPA);

and wherein said fourth program instructions are recorded on said medium (see *abstract and FIG.1-2 and 4-5 of Ashland*).

Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over "*Kuhn*" (US 6,023,765) in view of Clark et al. (US 7,237,119 B2, referred as "*Clark*" hereinafter).

As per Claim 1, KUHN discloses,

A computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: first program instructions to compare members within each of said groups to a list of trusted individuals (see for example, col.1, lines 23-29, *"assuming individual persons are first identified to the system in a satisfactory manner, their access to documents, programs, facilities, and other "objects" within the protected computer system is then controlled by a security system simply by comparing the user's name against a list of names of persons entitled to access the given object"*);

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (see *Equations (1) & (4) in* col.6; and for example, col.5, lines 65-67, "*Eq. (1) states, in effect, that human users are authorized to execute privilege assigned to a role only if they belong to the class of subjects authorized for that role*"; and col.6, lines 20-22, "*Equation (4) refers to privilege authorization: a subject can execute a privilege only if the privilege is authorized for a role in which the subject is currently active*");

third program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege (see *Equation (2) & (3) in* col.6; and for example, col.6, lines 7-15, "*Equation (2) refers to role assignment: a subject can execute a privilege only if the subject has been selected or been assigned an active role; and Equation (3) refers to role authorization: a subject's active role must be authorized for the subject*"); and

a computer readable medium; wherein said first, second and third program instructions are recorded on said medium (see for example, col.1, lines 12-13, *"The present invention relates to security in computer systems"*).

Kuhn does not explicitly disclose generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; and generate a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted.

However, in the same field of endeavor, Clark discloses a report generating mechanism for identifying member not on the list of trusted individuals and group name generally used for a group with user level privilege (see *FIG. 3-5 and 7*; and for example, col.3, line 37 to col.5, line 14 of Clark).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to incorporate the teachings of Clark in to the system of Kuhn, because both are in the fields of managing user authorization levels.

One having ordinary skill in the art would be motivated to modify the teachings of Kuhn to generate a report on the current status of members and group names because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, it would be obvious to modify Kuhn's system to generate a report using the user interface of Clark whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3 of Kuhn).

As per Claim 6, KUHN discloses,

A computer system for determining if any of a plurality of groups may have an improper actual level of privilege: means for comparing members within each of said groups to a list of trusted individuals (see *RBAC TRUSTED INTERFACE 40 in FIG.3 and USERS 26 and USER ID 28 in FIG. 2; where users are authorized by their user ids*; and for example, col.7, line 61 to col.8, line 14);

means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (see *(ROLE, PRIVILEGE) REQUEST 46 & RBAC TO MLS MAPPING FUNCTION 48 in FIG.3; and Equations (1) & (4) in* col.6); and

means for determining if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege (see *([COMPARTMENTS], LEVEL 50) in FIG.3; and Equation (2) & (3) in* col.6).

Kuhn does not explicitly disclose generate a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted; and

generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member.

However, in the same field of endeavor, Clark discloses a report generating mechanism for identifying member not on the list of trusted individuals and group name generally used for a group with user level privilege (see *FIG. 3-5 and 7*; and for example, col.3, line 37 to col.5, line 14 of Clark).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the teachings of Kuhn to generate a report on the current status of members and group names because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, it would be obvious to modify Kuhn's system to generate a report using the user interface of Clark whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3 of Kuhn).

As per Claim 11, KUHN discloses,

A computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: first program instructions to compare members within each of said groups to a list of trusted individuals (see for example, col.1, lines 23-29);

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (see *Equations (1) & (4) in* col.6);

third program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (see *Equation (2) & (3) in* col.6; and for example, col.6, lines 7-15); and

a computer readable medium; wherein said first, second and third program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Kuhn does not explicitly disclose generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; and

generate a report that said group with the higher actual privilege level has a group name not generally used for a group with the higher level privilege, such that the members of said groups with the higher actual privilege having a group name not generally used for a group with the higher level privilege are revealed as trusted or not trusted.

However, in the same field of endeavor, Clark discloses a report generating mechanism for identifying member not on the list of trusted individuals and group name generally used for a group with user level privilege (see *FIG. 3-5 and 7*; and for example, col.3, line 37 to col.5, line 14 of Clark).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the teachings of Kuhn to generate a report on the current status of members and group names because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, it would be obvious to modify Kuhn's system to generate a report using the user interface of Clark whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3 of Kuhn).

As per Claim 15, KUHN discloses,

A computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; first program instructions to compare members within each of said groups to a list of trusted individuals (see for example, col.1, lines 23-29);

second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (see *Equations (1) & (4) in* col.6);

and wherein said first and second program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Kuhn does not explicitly disclose remove said member not on the list of trusted individuals from said group. However, Clark discloses removing said member not on the list of trusted individuals from said group (see *Del Row in FIG. 4 & 7; and Level 140 in FIG.* 4; and for example, col.3, line 46 to col.4, line 23).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the RBAC system of Kuhn to remove said member not on the list of trusted individuals from said group, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, Kuhn's system removes said member not on the list of trusted individuals from said group whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3).

As per Claim 16, KUHN discloses,

A computer program product for managing privileges of groups, said computer program product comprising: first program instructions to determine if any group with an actual privilege level higher than

user level privilege has a group name on a list of group names generally used for a group with user level privilege or no privilege (see *Equation (2) & (3) in* col.6); and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with user level privilege or no privilege (see *Equations (1) & (4) in* col.6; and for example, col.5, lines 65-67), to compare members of such group to a list of trusted individuals (see for example, col.1, lines 23-29); and

a computer readable medium; wherein said first and second program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Kuhn does not explicitly disclose if any member(s) of such group do not appear on said list of trusted individuals, remove said member(s) from such group that do not appear on the said list of trusted individuals. However, Clark discloses removing said member not on the list of trusted individuals if any member(s) of such group do not appear on said list of trusted individuals (see *Del Row in FIG. 4 & 7; and Level 140 in FIG.* 4; and for example, col.3, line 46 to col.4, line 23).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the RBAC system of Kuhn to remove said member not on the list of trusted individuals from said group, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, Kuhn's system removes said member not on the list of trusted individuals from said group whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3).

As per Claims 2, 7 and 12, KUHN discloses,

wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances (see *ROLES 30 & OPERATIONS 32 in FIG. 3; and FIG. 5-6*);

and said third program instructions makes its determination separately for each application or application instance (see *PRIVILEGE SETS, PRIVILEGE SET & ROLE COMPARTMENT LEBELS in FIG. 6*); and means for determining if any group with an actual privilege level higher than user level privilege has a group name generally used for a group with user level privilege makes its determination separately for each application or application instance (see *RBAC TO MLS MAPPING FUNCTION 48 in FIG. 3*).

As per Claims 3 and 8, KUHN discloses,

fourth program instructions to determine if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (see *FIG.5 and PRIVILEGE SETS, PRIVILEGE SET & ROLE COMPARTMENT LEBELS in FIG. 6*); and means for determining if any groups with an actual privilege level higher than user level privilege have a group name not on a list of group names generally used for a group with the higher level privilege (see *RBAC TO MLS MAPPING FUNCTION 48 in FIG. 3*); and

and wherein said fourth program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Kuhn does not explicitly disclose generate a report that said group with the higher actual privilege level has a group name not generally used for a group with the higher level privilege, such that the members of said groups with the higher actual privilege having a group name not generally used for a group with the higher level privilege are revealed as trusted or not trusted.

One having ordinary skill in the art would be motivated to modify the teachings of Kuhn to generate a report on the current status of members and group names because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, it would be obvious to modify Kuhn's system to generate a report using the user interface of Clark whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3 of Kuhn).

As per Claims 4, 9 and 13, KUHN discloses,

wherein said second program instructions determine if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals (see for example, col.5, line 35 to col.7, line 60);

and means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals determines if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals (see *RBAC TO MLS MAPPING FUNCTION 48 in FIG. 3*).

Kuhn does not explicitly disclose generate a report that said group with the higher actual privilege level has all its members on the list of trusted individuals.

One having ordinary skill in the art would be motivated to modify the teachings of Kuhn to generate a report on the current status of members and group names because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, it would be obvious to modify Kuhn's system to generate a report using

the user interface of Clark whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3 of Kuhn).

As per Claims 5, 10 and 14, KUHN discloses,

fourth program instructions to determine: if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list of trusted individuals; if all the members of said group with the higher actual privilege having a group name not generally used for a group with higher level privilege are on the list of trusted individuals (see for example, col.5, line 35 to col.7, line 60); and

means for determining if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list of trusted individuals (see *RBAC TO MLS MAPPING FUNCTION 48 in FIG. 3*);

and wherein said fourth program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over "*Kuhn*" view of Morris et al. (EP 1 124 184 A2, referred as "*Morris*" hereinafter).

As per Claim 17, KUHN discloses,

A computer program product for managing privileges of groups, said computer program product comprising: first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege (see *Equation (2) & (3) in* col.6); and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level

higher than user level privilege (see *Equations (1) & (4) in* col.6; and for example, col.5, lines 65-67), to compare members of such group to a list of trusted individuals (see for example, col.1, lines 23-29); and

a computer readable medium; wherein said first and second program instructions are recorded on said medium (see for example, col.1, lines 12-13).

Kuhn does not explicitly disclose if any member(s) of such group do not appear on said list of trusted individuals, lower the actual privilege level of said group. However, Morris discloses lowering the actual privilege level of said group if any member(s) of such group do not appear on said list of trusted individuals (see *FIG. 1; and abstract*).

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to incorporate the teachings of Morris in to the system of Kuhn, because both are in the fields of controlling privilege levels.

One having ordinary skill in the art would be motivated to modify the RBAC system of Kuhn to lower the actual privilege level of said group if any member(s) of such group do not appear on said list of trusted individuals, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request. Therefore, Kuhn's system lowers the actual privilege level of said group lowers the actual privilege level of said group if any member(s) of such group do not appear on said list of trusted individuals by incorporating the privilege lowering teaching of Morris whenever the said mapping process is performed (see *abstract;* and *SUMMARY OF INVENTION* in col.3).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristine Kincaid
Kristine Kincaid
Supervisory Patent Examiner
AU 2139

Amare Tabor

AU 2139